Abstract: When large systems are attacked at multiple points, the attack profiles can be combined to help learn who the attackers are and what goals they are trying to achieve. This knowledge helps organizations focus their defensive efforts. However, validating intentionality models with real-world data is quite difficult (even when data is made available) as attackers and their network activities must be known. What is needed are realistic sets of synthetic data corresponding to both malicious and non-malicious network activity. In this presentation, we consider a range of synthetic modeling possibilities.

Bio: Doug Lundquist completed his PhD at the University of Illinois at Chicago in 2011, where he continues to pursue research. His research interests include: economic models for information search and discovery; smart pricing models for network usage; and cyber-security, focusing on semantic modeling and reconciliation of network attacks and defenses. He won a competition for innovative vehicle-to-vehicle communication technologies sponsored by US Department of Transportation. His work has been published in the International Journal of E-Business, Wireless Networks, and Personal and Ubiquitous Computing.